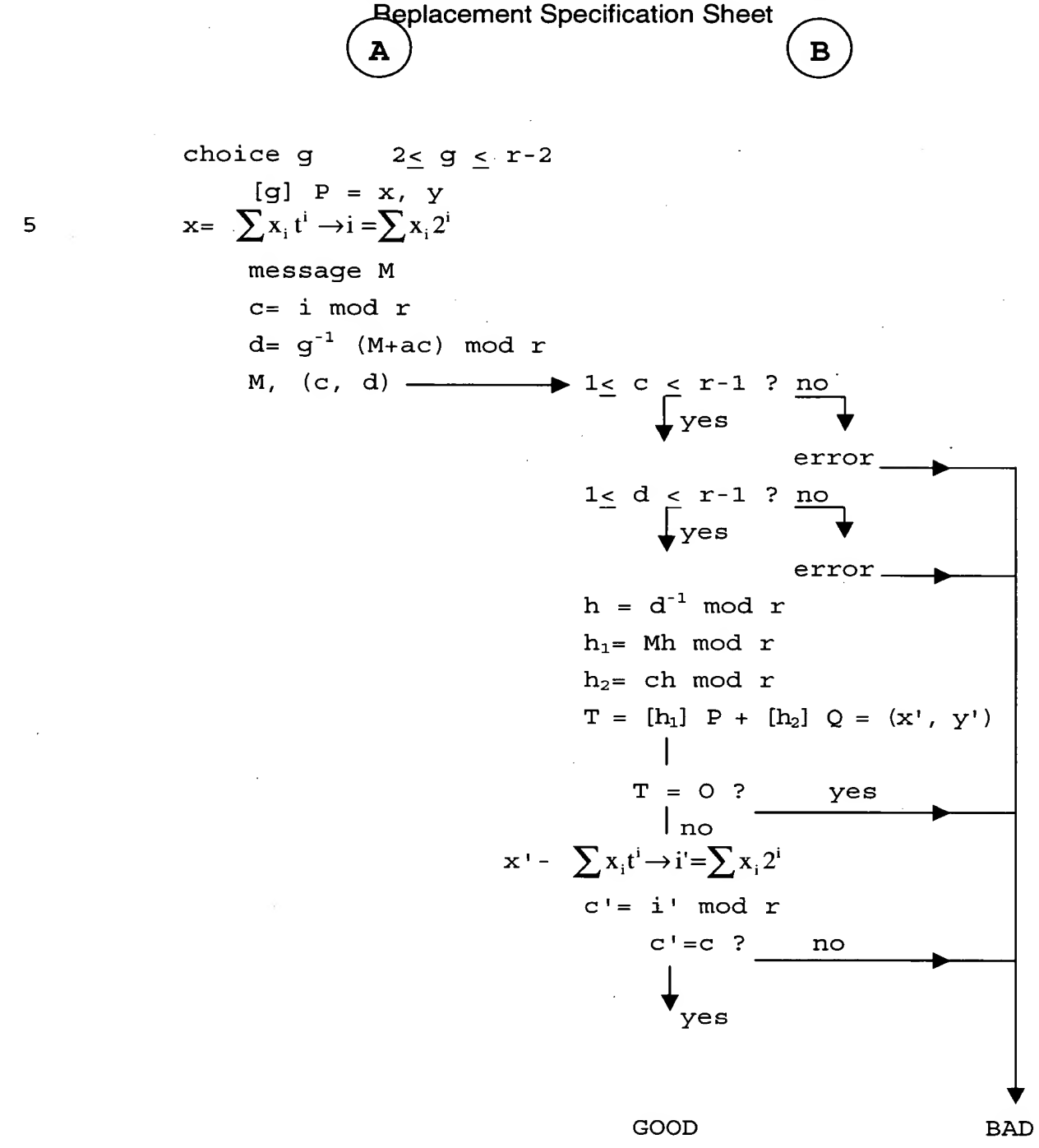
A
B
choice g 2≤ g ≤ r-2
[g] P = x, y
x= $\sum x_i t^i \rightarrow i = \sum x_i 2^i$
message M
c= i mod r
d= g^{-1} (M+ac) mod r
M, (c, d)
1≤ c ≤ r-1 ?
no
yes
error
1≤ d ≤ r-1 ?
no
yes
error
h = d^{-1} mod r
h_1= Mh mod r
h_2= ch mod r
T = [h_1] P + [h_2] Q = (x', y')
T = O ?
yes
no
x'- $\sum x_i t^i \rightarrow i' = \sum x_i 2^i$
c'= i' mod r
c'=c ?
no
yes
GOOD
BAD